《健康信息学　公钥基础设施　第3部分：认证机构的策略管理》国家标准编制说明

一、工作简况

（一）任务来源

本文件的制订计划由中国标准化研究院提出，经国家标准委批准，正式列入 2023 年推荐性国家标准制修订项目计划，项目编号为20233826-T-424，采标号为ISO 17090-3:2021，项目名称为《健康信息学　公钥基础设施　第3部分：认证机构的策略管理》。

本文件的起草单位包括：中国标准化研究院、中国人民解放军总医院、北京航空航天大学、上海中医药大学、深圳市卫生健康发展研究和数据管理中心、福建省中科标准科技有限责任公司、浙江大学、浙江师范大学、北京信息科技大学、厦门市众科佰联标准化服务有限公司、福建理工大学等。

（二）本文件制定目的和意义

随着经济社会的快速发展，公众对健康的关注不断提升，对多样化的健康服务需求日益增长。健康信息系统作为医疗卫生改革的核心，能够整合社会健康资源，提升服务效率，促进健康服务的形式、流程和内容的根本变革，提高健康资源的可及性和公平性，有效缓解就医难、就医贵的问题。

互联网虽然提供了便捷的信息交换手段，但其不安全性要求我们采取措施保护信息的私密性和保密性。数字证书通过绑定技术、策略和管理过程，利用公钥密码算法和证书确认身份，保障敏感数据在不

安全环境中安全交换。在健康领域，数字证书技术通过鉴别、加密和数字签名等手段，确保个人健康记录的安全访问和传输，满足临床和管理的需求，同时也强调了互操作性的重要性，以支持跨组织和辖区的健康信息交换。制定一系列能够统一健康信息化相关的业务和技术问题，规范信息交换、共享的各个环节的基础性、通用性的技术标准至关重要。

通过修订《健康信息学　公钥基础设施　第 3 部分：认证机构的策略管理》，旨在适应信息技术的快速发展，提高医疗数据处理的安全性和效率。这一标准的更新有助于加强对患者隐私的保护，优化认证流程，确保健康信息在传输和存储过程中的安全性和完整性，同时促进不同医疗机构间的互操作性和信息共享。这些改进对于维护医疗保健领域的数据安全和提升服务质量至关重要。

（三）主要工作过程

3.1 成立起草组，确定标准框架并形成标准草案稿

2024 年 2 月——5 月，在中国标准化研究院的组织下，成立了由中国标准化研究院、中国人民解放军总医院、北京航空航天大学、上海中医药大学、深圳市卫生健康发展研究和数据管理中心、福建省中科标准科技有限责任公司、浙江大学、浙江师范大学、北京信息科技大学、厦门市众科佰联标准化服务有限公司、福建理工大学等单位组成的标准起草组。

因为本文件是修改采用国际标准，所以起草工作小组前期对 ISO 17090-3：2021《健康信息学　公钥基础设施　第 3 部分：认证机构

的策略管理》进行了认真的翻译研究工作，并对国际标准中引用到的标准和技术文件逐一进行了查阅和研究，初步确定了本文件的草案第一稿。

在上述工作基础上，起草组在对国内外的健康信息系统建设中的信息安全建设与应用情况进行了资料调研和分析，确立了标准框架和具体内容，形成标准草案正式稿。

3.2 确定标准草案并形成征求意见稿

2024 年 6 月——9 月，在确立的草案稿的基础上，起草组内部经过多次讨论后对标准的技术内容进行了充实和完善。同时，起草组多次组织国内相关的专家学者召开研讨会，对标准框架及草案内容提出进行研讨。起草组在广泛听取专家的意见和建议，并经过多次内部的研讨、修改后，于 2024 年 9 月形成了标准的征求意见稿。

二、国家标准编制原则和确定国家标准主要内容的论据

（一）编制原则

本文件按照 GB/T 1.1-2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》和 GB/T 1.2-2020《标准化工作导则　第 2 部分：以 ISO/IEC 标准化文件为基础的标准化文件起草规则》的要求，采用翻译法修改采用 ISO 17090-3：2021《健康信息学　公钥基础设施　第 3 部分：认证机构的策略管理》。同时充分考虑到现阶段我国健康信息系统建设情况和实际需求，使其具有可操作性。

（二）确定论据

本文件修改采用国际标准 ISO 17090-3：2021《健康信息学　公

钥基础设施　第 3 部分：认证机构的策略管理》。

（三）主要内容

1 缩略语

本文件定义的缩略语包括：属性机构、认证机构、证书策略、认证操作声明、证书撤销列表、对象标识符、公钥证书、公钥基础设施、注册机构、可信第三方。

2 医疗保健环境中数字证书策略管理要求

本章节给出了医疗保健环境中数字证书策略管理的要求，强调了在医疗保健领域中，数字证书的部署必须确保个人健康信息通信的安全性。还提出了对健康应用软件所需安全服务的高层保证、基础设施的高可用性、信任要求、互联网兼容性以及便于评估和比较认证策略（CP）的要求。这些要求确保了医疗保健信息的安全传输，支持跨国家和区域界限的信息交换，并加速了对医疗保健 CA 的信任过程。

3 医疗保健 CP 和 CPS 的结构

本章节主要介绍了医疗保健领域中数字证书政策（CP）和证书实践声明（CPS）的结构和要求。强调了认证机构（CA）在签发证书时必须遵循的注册、鉴别、分发、撤销和密钥管理等方面的政策和程序。也讨论了 CP 和 CPS 之间的关系，以及它们如何帮助证书持有者和可依赖方理解证书的可信度。

4 医疗保健 CP 的最小要求

本章节详细讨论了医疗保健领域中证书政策（CP）的最小要求。这些要求包括证书的发布和存储责任、标识和鉴别过程、以及证书生

命周期操作请求。以及证书的申请、处理、签发、接受、使用、更新、修改、撤销和暂停等证书生命周期的各个阶段。强调了医疗保健领域中数字证书政策（CP）的物理、程序和人员控制，以及技术方面的安全控制。规范了医疗保健领域中数字证书政策（CP）的法律和业务相关问题。

5 PKI 公开声明模型

本章节介绍了 PKI 公开声明模型，并提供了一个结构示例表格，以展示应该公开哪些信息。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

本文件的技术内容不涉及试验验证的要求，通过本文件的实施将能够推动外科手术术语系统的统一，保障数据融合、汇交和统计分析。

四、采用国际标准和国外先进标准的程度

本文件修改采用国际标准 ISO 17090-3：2021《健康信息学　公钥基础设施　第 3 部分：认证机构的策略管理》

五、与有关的现行法律、法规和强制性国家标准的关系

本文件符合国家现行法律、法规、规章和强制性国家标准的要求。

六、重大分歧意见的处理经过和依据

本文件在制定过程中未出现重大分歧意见。

七、国家标准作为强制性国家标准或推荐性国家标准的建议

本文件建议作为推荐性标准发布实施。

八、贯彻国家标准的要求和措施建议

本文件作为推荐性标准，建议首先利用报纸、电视、电台及微信、微博等各种新媒体，加大宣传力度，为标准的实施营造良好的社会氛围。其次在有影响力的医疗服务平台中应用实施。同时，将实施过程中出现的问题和好的改进建议反馈给标准起草组，以便未来对本文件的继续修订和完善。

九、废止现行有关标准的建议

本文件不涉及对现行标准的废止。

十、其他

无。

《健康信息学　公钥基础设施　第3部分：认证机构的策略管理》

国家标准起草组

2024年9月